UNIVERSITY OPERATING PROCEDURE

Title: Controlled Unclassified Information (CUI)

Overview

The Federal Government requires that entities safeguard certain categories of information. There are some categories that are covered by other federal, state, or international laws (i.e., protected health information under HIPAA, student record data under FERPA, non-public personal information under GDPR). In addition to existing federal regulations, federal agencies (i.e., Department of Defense (DoD), National Institutes of Health (NIH)) may identify certain information as "Controlled Unclassified Information", or CUI, that requires additional protections. Those units, departments, or individuals who receive CUI from a federal agency are required to safeguard and secure CUI. While most CUI is related to research, CUI could also be received, created, or shared in connection with university activities unrelated to research. Examples of how the University could receive or exchange CUI include, but are not limited to, contractual obligations, grants or awards, non-disclosure agreement requirements, data use agreements, or other agreement or arrangement. It is the responsibility of the federal agency to designate CUI and to communicate this to the University recipient(s).

Applicability of the Procedure

This UOP applies to all administrative and academic units, employees, students, volunteers, contractors, and affiliates that collect, access, use and/or disclose Controlled Unclassified Information (CUI).

Definitions

Controlled Unclassified Information (CUI): Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

Covered Agencies: Federal executive branch agencies, including but not limited to the Department of Defense, the Department of Health & Human Services, and the National Institutes of Health, that handle CUI as well as all organizations and entities (which includes universities) that handle, possess, use, share, create, or receive CUI. Or which operate, use, or have access to Federal information and information system on behalf of a federal agency.

Covered Persons: means all UVM faculty, staff, students, affiliates, contractors, visitors, volunteers, subcontractors, and third-parties employees and agents) who collect, access, use, and/or disclose CUI on behalf of the University of Vermont.

CUI Implementing Regulations: 32 CFR 2002 and related implementing regulations including, but not limited to, DFARs 252.204-7012.

Information Security Plan (ISP): is a plan developed by the Covered Person(s) in consultation with Enterprise Technology Services (ETS) to maintain the confidentiality, privacy, and security of CUI.

NIST Special Publication 800-171: NIST SP 800-171 is a NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI).

Procedures

UVM Covered Persons are required to protect and safeguard all CUI in accordance with this University Operating Procedure (UOP), with UVM's Information Security Policy, Information Security Procedure, and Privacy Policy as well as with any CUI Implementing Regulations and any applicable information security plans, contracts, and agreements.

As required by the federal government, CUI can only be stored and processed on IT systems that have been risk assessed to comply with NIST SP 800-171 standards. Therefore, UVM Covered Persons who wish to engage in an activity involving CUI can only do so within the approved CUI environment. Access will need to go through SPA (for research) and/or your IT support in conjunction with Enterprise Technology Services (ETS). Covered Persons are required to adhere to any information security plans associated with CUI from receipt through destruction.

There are many different types of CUI. A list of CUI organizational groupings and specific CUI categories can be found in the Federal Archives. Organizational groupings include critical infrastructure, defense, export control, financial, immigration, intelligence, international agreements, law enforcement, legal, natural, and cultural resources, North Atlantic Treaty Organization (NATO), nuclear, patent, privacy, procurement and acquisition, proprietary business information, provisional, statistical, tax, and transportation. Within these broad groupings are specific categories including data related to homeland security, national infrastructure, nuclear and intelligence. Individual federal agencies are required to develop and issue regulations that provide details on how they will implement the CUI requirements.

While most work with CUI will be attached to awards that are administered through Sponsored Project Administration (SPA) and, therefore, SPA will assist with identifying projects where CUI will be used and connect the researchers to the Information Security Officer to develop a ISP where needed and/or will work with the researchers as it relates to handling, storing and use of CUI, CUI may enter the University outside of the scope of SPA. Ultimately, individual researchers who use CUI are responsible for complying with UVM's related Policies, UOPs and federal and state regulations.

Failure to comply with the CUI Implementing Regulations, UVM's policies and procedures, and any applicable information security plans, contracts and agreements may result in contractual, financial and legal penalties to UVM and to the individual(s) involved, including administrative sanctions such as loss of federal funding and loss of future awards/grants. In addition, violations can result in disciplinary action including termination or expulsion from UVM.

Given the sensitivity and risk, any known or suspected mishandling of any protected data, including CUI, must be reported without delay. Reports may be made via the Compliance and Ethics Reporting and HelpLine (the Compliance HelpLine). The Compliance Helpline accepts anonymous reports.

Contacts

Questions concerning the daily operational interpretation of this UOP should be directed to the following:	
Title(s)/Department(s):	**Contact Information:**
Office of the Vice President for Research	www.uvm.edu/ovpr/contact_us_0 (802) 656-2918
Research Integrity	www.uvm.edu/ovpr/contact-research-integrity (802) 656-1329
Information Security Officer	iso@uvm.edu (866) 236-5752
Chief Privacy Officer	privacy@uvm.edu (802) 656-3086

Forms/Flowcharts/Diagrams

- None

Related Documents/Policies

- 32 CFR 2002
- DFARs 252.204-7012
- Export Controls Policy
- Federal Archives – Categories of CUI
- Information Security Policy
- Information Security Procedure
- NIST SP 800-171
- Privacy Policy
- SPA Review Procedure for Controlled Unclassified Information

Training/Education

Training related to this policy is as follows:

Training Topic:	Handling and Safeguarding CUI		
Training Audience:	All Covered Persons	**Delivered By:**	Research Integrity
Method of Delivery:	On-Line	**Frequency:**	Prior to Accepting CUI

Training Topic:	Handling and Safeguarding CUI – Refresher		
Training Audience:	All Covered Persons	**Delivered By:**	Research Integrity
Method of Delivery:	On-Line	**Frequency:**	Annually Throughout Life of CUI (until destruction)

About This Procedure

Responsible Official:	Chief Information Officer	**Approval Authority:**	Chief Information Officer
Affiliated Policy Number(s):	V.1.7.2, V.9.2.4, UOP14	**Effective Date:**	October 3, 2022
Revision History:	None		

University of Vermont Policies and Operating Procedures are subject to amendment. For the official, approved, and most recent version, please visit UVM's Institutional Policies Website.